VITO PLANTAMURA

LA TUTELA PENALE DEI DATI PERSONALI

SOMMARIO: 1. Considerazioni introduttive. — 2. Il c.d. codice della *privacy*. — 3. *Excursus* sulle violazioni amministrative. — 4. Gli illeciti penali posti a tutela delle funzioni del Garante. — 5. L'illecito trattamento dei dati personali. — 6. Brevi cenni comparatistici. — 7. Rilievi conclusivi.

1. Considerazioni introduttive.

Se è vero che il primo aspetto emerso, in riferimento al bene *privacy*, è stato quello, prettamente individuale, consistente nell'ottocentesco « *right to be let alone* », è altrettanto indiscusso che, se pur in epoca successiva, a questo se ne è affiancato uno ulteriore, avente una dimensione più propriamente *sociale*, rappresentato, in definitiva, dall'interesse al controllo sul corretto trattamento dei dati personali[1].

D'altronde, la spiccata vocazione sociale della tutela dei dati personali era apparsa già dalla disciplina contenuta in una legge « pionieristica » europea, ovverosia la *Bundesdatenschutzgesetz* tedesco-occidentale del 1977[2], nella quale, essendo stati previsti diritti di accesso, correzione, e financo cancellazione dei dati, in definitiva, si era voluto statuire un vero e proprio *diritto all'informazione* sui dati personali medesimi, il cui riconoscimento aveva confermato l'aspetto, appunto, sociale assunto dalla *privacy* in rapporto ai *computers*[3].

Tale aspetto, inoltre, era risultato ampiamente anche dalle vicende che avevano portato, in Francia, alla emanazione di un'altra delle prime leggi europee in materia — la n. 78-17 del 1978 « *Loi relative à l'informatiques, aux fischiers et aux libertés* »[4] —, come *reazione* alla precedente approva-

[1] Cfr. Patrono, *Privacy e vita privata*, in *Enc. dir.*, Milano, 1986, 559.

[2] Sul versante strettamente penalistico, però, i reati previsti in tale legge erano stati criticati, per via del loro *deficit* di determinatezza, da Tiedemann, *Criminalità da computer*, in *Pol. dir.*, 1984, 614. Ed è forse anche per questo che poi, in sede di riforma della legge in questione, il legislatore tedesco aveva deciso di puntare sui rimedi civilistici, prevedendo: un diritto all'indennizzo che prescindeva dalla prova della colpa; nonché, nei casi di particolare gravità, la facoltà di richiedere, se pur in via equitativa, il risarcimento del danno non patrimoniale. Sul punto, si veda Manna, *Tutela penale della personalità*, Bologna, 1993, 137 s.

[3] In questo senso, si era espresso Manna, *Beni della personalità e limiti della protezione penale*, Padova, 1990, 348.

[4] Cfr. Manna, *Beni della personali-*

zione di un disegno di legge governativo — poi abbandonato —, relativo alla realizzazione del famigerato « progetto Safari » (*Système automatisé pour les fischiers administratifs e le rèpertoire des individus*), con il quale il governo dell'epoca si era proposto, tramite i nuovi mezzi elettronici, di schedare l'intera popolazione francese, anche attribuendo, ad ogni cittadino, un numero identificativo.

Storicamente, quindi, il secondo citato aspetto della *privacy* si è sviluppato, soprattutto, a seguito dell'evolversi della tecnologia, e, in particolare, della « nascita » dell'informatica, la quale, chiaramente, consente di gestire, con relativa facilità, anche una enorme quantità di dati. Il nesso, tra lo sviluppo dell'informatica ed il crescente interesse per le modalità di gestione dei dati personali, è inoltre dimostrato, da un lato, dall'originario riferimento al trattamento *automatizzato* dei dati contenuto nella versione iniziale della succitata legge francese, e, dall'altro, dalla circostanza che, nella prima Carta costituzionale europea, in cui è stata presa in considerazione la protezione dei dati personali, ovverosia quella portoghese del 1976[5], la tutela in questione — *ex* art. 35 — è stata riferita esclusivamente al trattamento *informatizzato* dei dati stessi, per altro, nel più ampio ambito della regolamentazione dell'utilizzo, solo per fini socialmente utili, dell'informatica: ambito che, del resto, caratterizza anche il disposto di cui all'art. 18 co. 4, della Costituzione spagnola del 1978[6].

Da questo punto di vista, dunque, in netta controtendenza si è posta la successiva direttiva 95/46/CE, sulla protezione dei dati personali, la quale, al suo art. 2 lett. *b*), fa rientrare, nel concetto di trattamento di dati rilevante, ai sensi della direttiva medesima, quello svolto « *con o senza l'ausilio di processi automatizzati* », così sganciando, quantomeno a livello di previsione astratta, la protezione dei dati personali dal concetto di « riservatezza informatica », e facendo ipotizzare, da parte di attenta dottrina, una sorta di processo circolare di derivazione dei beni giuridici, per cui, se dal bene tradizionale dell'onore, storicamente, è derivato quello della *privacy*, ora sembrerebbe quasi che da quest'ultima, nel suo aspetto più avanzato, relativo alla protezione dei dati personali *anche se non trattati elettronicamente*, stia derivando una forma più allargata, e dunque ancor meno determinata, di tutela dell'onore[7].

Anche queste considerazioni inducono a ritenere che, come emergerà più chiaramente nel proseguo della trattazione, soprattutto da un punto di vista penalistico, forse sarebbe meglio limitare la tutela dei dati personali a quelli c.d. *sensibili*, perché tale protezione appare ovviamente strumentale a garantire l'uguaglianza dei cittadini — come previsto, ad esempio, dall'art. 3 co. 1 della nostra Costituzione — « *senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni*

---

tà…, *cit.*, 350 ss. Per un riferimento anche alla nuova versione della legge in questione, la quale, attraverso le modifiche operate dalla loi n. 2004/801, del 2004, è stata finalmente adeguata, dopo un *iter* legislativo particolarmente lungo e macchinoso, alla direttiva 95/46/CE, si veda GUERRINI, *Prime osservazioni in margine alla nuova legge francese sulla protezione dei dati personali*, in questa *Rivista*, 2004, 645 ss.

[5] Cfr. *www.parlamento.pt*

[6] Cfr. *www.constitucion.es*

[7] Cfr. P. VENEZIANI, *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali*, in AA.VV., *Il diritto penale dell'informatica nell'epoca di internet*, a cura di PICOTTI, Padova, 2004, 183 ss., e, spec., 193 ss.

personali e sociali », e dunque risulta più solidamente agganciata ai valori fondamentali su cui si basano le moderne società democratiche. Come ribadito, per altro, anche dal comma terzo del citato art. 35 della Carta costituzionale portoghese, secondo il quale l'informatica non può essere utilizzata per il trattamento dei dati che si riferiscono alle convinzioni filosofiche o politiche, all'appartenenza partitica o sindacale, alla fede religiosa, alla vita privata e all'origine etnica, salvo che vi sia l'espresso consenso del titolare dei dati medesimi. E questo, appunto, come garanzia di non discriminazione.

2. Il c.d. codice della *privacy*.

Avendo svolto le precedenti osservazioni preliminari, si può ora entrare nel vivo della trattazione, iniziando col ricordare che in Italia, attualmente, il decreto legislativo del 30 giugno 2003, n. 196, meglio noto, appunto, quale codice della *privacy*, si apre, al suo primo articolo, con l'enunciazione di un principio — che non trova riscontro nella L. n. 675/96, che in precedenza regolava la medesima materia — in virtù del quale « *chiunque ha il diritto alla protezione dei dati personali che lo riguardano* ». Tanto è vero che, in sede di relazione al D.Lgs. di cui trattasi, si è ritenuto di specificare che « *l'art. 1 introduce nell'ordinamento il diritto alla protezione dei dati personali, diritto fondamentale della persona, autonomo rispetto al più generale diritto alla riservatezza, già richiamato dall'art. 1 della legge n. 675/1996* »[8].

Conseguentemente, *ex* art. 2 co. 1, tale codice ha, come sua finalità, quella di garantire che il *trattamento dei dati personali* si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità degli interessati — ovverosia, *ex* art. 4 lett. *i*), delle persone fisiche, delle persone giuridiche, degli enti o delle associazioni, cui si riferiscono i dati personali —, con particolare riguardo alla riservatezza, all'identità personale ed al diritto alla protezione dei dati.

Allo stesso tempo, però, il codice di cui trattasi si prefigge anche di garantire che i molteplici diritti riconosciuti, *ex* art. 7, agli interessati in questione — tra cui quello di accesso ai dati, di modifica e/o aggiornamento degli stessi, nonché, in alcuni casi, di opposizione al trattamento dei medesimi —, possano essere esercitati con modalità tali da risultare rispettose dei principi di semplificazione, armonizzazione ed efficacia. Deve aggiungersi, poi, che, con la previsione di nozioni davvero particolarmente ampie — già proprie, del resto, pure della legge precedente —, il codice in questione, da un lato — *ex* art. 4 lett. *b*) —, definisce « dato personale » qua-

[8] Cfr. Manna, *Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali*, in questa *Rivista*, 2003, 229 s. Inoltre, sempre per un commento dei profili sanzionatori della nuova disciplina della *privacy*, si rinvia a: Castaldo, *Illeciti penali*, in AA.VV., *La nuova disciplina della privacy*, comm. diretto da Sica-Stanzione, Bologna, 2004, 740 ss.; Corrias Lucente, *La nuova normativa penale a tutela dei dati personali*, in Cardarelli-Sica-Zeno Zencovich, *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 631 ss.; Manna, *Codice della* privacy*: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali*, in *Dir. pen. proc.*, 2004, 15 ss.

lunque informazione attinente a persone fisiche o giuridiche, enti o associazioni, identificati, o anche solo identificabili, perfino indirettamente, mediante riferimento a qualsiasi altra informazione, *ivi* compresi i numeri di identificazione personale, e, dall'altro — *ex* art. 4 lett. *a*) —, intende per « trattamento » qualunque operazione, semplice o complessa, effettuata, si badi, pure *senza l'ausilio di strumenti elettronici*, concernente la raccolta di dati, anche se non registrati in una banca dati, o la loro registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e distruzione. Decisamente più convincente, invece, proprio perché meglio circoscritta, appare la definizione, cui si è accennato in precedenza, di dati sensibili, nel novero dei quali — *ex* art. 4 lett. *d*) — rientrano solo quelli idonei a rivelare: l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché lo stato di salute e la vita sessuale.

Ebbene, la prima osservazione che può formularsi circa le definizioni summenzionate è, sicuramente, che le stesse estendono (forse inopinatamente) la protezione della *privacy*/riservatezza anche alle persone giuridiche, agli enti ed alle associazioni. Mentre, sia la citata direttiva 95/46/CE, sulla protezione dei dati personali, che la successiva direttiva 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, limitano il concetto di « dato personale » alle informazioni relative alle *persone fisiche*. Limitazione che, del resto, è propria tanto della citata legge francese in materia, quanto di quella spagnola (legge organica n. 15/99)[9]. E questo non a caso.

Sono solo quest'ultime, infatti, ad avere una loro « vita privata », e se è vero che tale espressione risente di un certo margine di inafferrabilità, come dimostra la controversa previsione della fattispecie incriminatrice di cui all'art. 615-*bis* c.p. — che punisce le interferenze illecite, appunto, nella vita privata[10] —, non si può comunque seriamente dubitare che la stessa risulti inapplicabile a soggetti diversi dalle persone fisiche, non foss'altro per la frequente previsione contestuale della tutela della vita privata e *familiare*.

Inoltre, altrettanto criticamente, si deve rilevare che il legislatore italiano — questa volta, però, come accennato, in ossequio a quanto previsto in sede europea — ha scelto di applicare la stessa identica disciplina prevista per il trattamento automatizzato di dati, anche a quello eventualmente posto in essere senza l'ausilio di strumenti elettronici. Tuttavia, senza incorrere in un contrasto con la più volte menzionata direttiva, che non specificava il tipo e la natura delle sanzioni che gli Stati avrebbero dovuto prevedere, almeno in sede penale, ben si sarebbe potuta limitare

---

[9] Cfr. *http://noticias.juridicas.com*. Su tale legge, si veda FROSINI, *La nuova legge spagnola sulla protezione dei dati personali*, in questa *Rivista*, 2000, 769 ss.

[10] In argomento, si rinvia a: MANNA, *Riservatezza, arte, e scienza: quid iuris?*, in questa *Rivista*, 1986, 510 ss.; ID., *Beni della personalità...*, *cit.*, 294 ss.; PLANTAMURA, *Moderne tecnologie, riservatezza e sistema penale: quali equilibri?*, in questa *Rivista*, 2006, 417 ss.; KAPUN, *L'abuso degli mms è passibile di condanna penale*, in *Dir. pen. proc.*, 2006, 1013 ss.

l'operatività delle fattispecie incriminatrici alle sole ipotesi di trattamento *automatizzato* dei dati, che ovviamente sono relative ad un numero di dati assai maggiore. E questo proprio coerentemente con il valore meta-individuale *sociale*, che la *privacy* tende ad assumere, appunto, in riferimento al profilo della tutela dei dati personali[11]. D'altronde, anche da un punto di vista strettamente penalistico, la prospettiva della protezione di un bene decisamente collettivo, comunque emerge dalla scelta operata dal nostro legislatore — prima con la L. n. 675/96[12], e, dopo, con il D.Lgs. n. 196/2003 — di prevedere la procedibilità d'ufficio, non solo dei reati posti a tutela della funzione svolta — in piena autonomia e con indipendenza di giudizio e di valutazione (art. 153 del codice) — dal Garante della *privacy*[13], ma perfino del delitto di trattamento illecito di dati, che protegge direttamente il bene *privacy*, ma, come chiarito, appunto nella sua dimensione meta-individuale sociale. Mentre, è solo quando la *privacy* assume una dimensione squisitamente individuale, come succede, in modo paradigmatico, nel citato art. 615-*bis* c.p, che, di conseguenza — come avviene, ovviamente, anche nel caso dei delitti contro l'onore —, è statuita la procedibilità a querela della persona offesa.

3. *Excursus* sulle violazioni amministrative.

Nel codice della *privacy*, il ricorso alla sanzione amministrativa risulta assai circoscritto, perché, le violazioni ritenute espressive di un disvalore più grave risultano presidiate da sanzioni penali, mentre, la reazione avverso quelle più lievi, è affidata ai poteri coercitivi propri del Garante (artt. 142 e 143)[14]. In definitiva, quindi, le violazioni amministrative seguono un doppio binario di tutela, da un lato, cioè, sono utilizzate per prevenire e punire le condotte di ostacolo all'attività istruttoria del Garante stesso, mentre, dall'altro, sono dirette a garantire l'osservanza di quelle norme procedurali ispirate, a loro volta, alla garanzia dei diritti individuali degli interessati[15].

Più in particolare, l'art. 161 punisce l'omessa — o, comunque, inidonea — informativa all'interessato, in violazione dell'art. 13, con la san-

[11] Cfr. Manna, *Beni della personalità...*, *cit.*, 332 ss.

[12] In riferimento alla normativa precedente, critica la scelta della procedibilità d'ufficio, anche perché la *privacy* del soggetto potrebbe essere ulteriormente lesa dal c.d. *strepitus fori*, Cagli, *La rilevanza del consenso nella disciplina del trattamento dei dati personali*, in AA.VV., *Il diritto penale dell'informatica...*, *cit.*, 277 ss., e, spec., 298.

[13] Anche sul ruolo del Garante, nonché, più in generale, sui profili amministrativi della tutela dei dati, da ultimo si veda Lacava, voce *Dati personali (dir. amm.)*, in *Diz. dir. pubbl.*, Milano, 2006, 1710 ss., e, spec., 1715 ss.

[14] Per completezza, si deve menzionare che, oltre al procedimento per reclamo al Garante, di cui al citato art. 142, l'interessato, nel caso in cui voglia far valere il proprio diritto d'accesso, o un altro diritto previsto sempre dall'art. 7, può proporre ricorso (art. 145), a sua scelta, dinanzi al Garante o all'Autorità giudiziaria. Inoltre, dev'essere ricordato anche il disposto dell'art. 15, secondo il quale « *1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. 2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11* », che dispone le modalità di trattamento dei dati personali.

[15] Cfr. Manna, *Il quadro sanzionatorio...*, *cit.*, 72 ss.

zione amministrativa del pagamento di una somma da tremila a diciottomila euro, prevedendo, altresì, sanzioni più gravi, nel caso di dati sensibili, giudiziari o il cui trattamento — *ex* art. 17 — presenta rischi specifici, nonché, in ogni altro caso in cui il pregiudizio degli interessati sia stato di speciale rilevanza. Inoltre, le somme in questione possono essere aumentate fino al triplo qualora, in ragione delle condizioni economiche del soggetto responsabile, se irrogate nella loro misura base, risulterebbero ineffettive.

Altre analoghe fattispecie sono previste dall'art. 162. Tale articolo, al suo primo comma, sanziona, con il pagamento di una somma da cinquemila a trentamila euro, la cessione dei dati non solo, specificamente, in violazione di quanto previsto dall'art. 16 co. 1 lett. *b*) — secondo il quale, nel caso di cessazione del trattamento, i dati possono essere ceduti ad altro titolare, purché siano destinati ad un trattamento compatibile con lo scopo per cui, in precedenza, erano stati raccolti —, ma anche, più in generale, in violazione di qualsiasi altra disposizione in materia di disciplina del trattamento dei dati personali. Lo stesso articolo, poi, al suo secondo comma, punisce, con la sanzione pecuniaria da cinquecento a tremila euro, la comunicazione, all'interessato — o, in casi di incapacità, ad un suo prossimo congiunto —, dei suoi dati personali idonei a rivelarne lo stato di salute, compiuta in violazione del disposto di cui all'art. 84 co. 1, secondo il quale tale comunicazione può essere effettuata, da parte di persone esercenti le professioni sanitarie e di organismi sanitari, solo per il tramite di un medico designato dall'interessato medesimo o dal titolare del trattamento.

L'art. 163 punisce, invece, l'omessa o incompleta notificazione del trattamento dei dati al Garante prevista dall'art. 37 — o, comunque, la notificazione effettuata in violazione delle modalità di cui all'art. 38 —, con il pagamento di una somma da diecimila a sessantamila euro e con la sanzione accessoria — *ex* art. 165, invece, prevista solo come eventuale, nei casi di violazione degli artt. 161 e 162 — costituita dalla pubblicazione dell'ordinanza ingiuntiva, per intero o per estratto, in uno o più giornali indicati nel provvedimento stesso.

Nel codice, quindi, giustamente è stata confermata la scelta di escludere, dalla tutela penale, l'omessa o incompleta notificazione al Garante, scelta che già era stata espressa con l'art. 12 del D.Lgs. n. 467/01 (Disposizioni correttive e integrative della normativa in materia di dati personali), il quale aveva sostituito il disposto di cui all'art. 43 L. n. 675/96, inserendo, appunto, l'illecito amministrativo di « *Omessa o incompleta notificazione* », al posto del precedente delitto di « *Omessa o infedele notificazione* ».

Sempre a tutela della funzione istruttoria del Garante, si pone, in chiusura del novero degli illeciti amministrativi previsti, quello, statuito dall'art. 164, e sanzionato con la pena pecuniaria da quattromila a ventiquattromila euro, di omessa informazione o esibizione al Garante. Tale fattispecie si applica nel caso in cui il Garante stesso, a seguito della presentazione di un ricorso (art. 150), o *sua sponte* (art. 157), abbia richiesto al titolare o al responsabile del trattamento, all'interessato, o anche a terzi, di fornire informazioni e/o di esibire documenti, e il soggetto richiesto abbia appunto omesso di fornire e/o esibire quanto richiestogli.

Ebbene, in conclusione di questo breve *excursus*, non ci si può esimere dal tratteggiare alcune prime prospettive *de iure condendo*, relative alla

tutela amministrativa. In primo luogo, si deve sottolineare come sia auspicabile che, in futuro, gli illeciti amministrativi siano puniti anche con sanzioni interdittive, e non più solo con quelle pecuniarie. Inoltre, come emergerà più ampiamente nel corso del prossimo paragrafo, è lo stesso ambito dell'illecito amministrativo che, in una prospettiva di riforma, dovrebbe essere ampliato: ma solo *verso l'alto*. Non cioè, predisponendo una tutela amministrativa di quelle violazioni lievi, che oggi, come accennato, rientrano nell'area di competenza del Garante, ma, piuttosto, in virtù di un'opera di radicale depenalizzazione dei reati posti a tutela delle funzioni del Garante medesimo.

4. Gli illeciti penali posti a tutela delle funzioni del Garante.

Avendo succintamente trattato degli illeciti amministrativi, adesso si deve passare ad analizzare, altrettanto brevemente, le fattispecie incriminatrici poste a tutela del corretto adempimento delle funzioni svolte dal Garante. D'altronde, è innegabile che tali fattispecie — così come, del resto, gli illeciti amministrativi fin qui considerati — certamente non « affollano » i repertori giurisprudenziali, dando la sensazione di una certa *sproporzione*, tra il corposo impianto normativo del codice, e le reali esigenze di protezione dei dati personali, che forse, nonostante il processo di sensibilizzazione in corso, non sono poi così sentite da parte dei consociati.

Ebbene, il primo di tali reati è quello previsto dall'art. 168, il quale — salvo che il fatto costituisca un più grave reato — punisce, con la reclusione da sei mesi a tre anni, chiunque, nelle notificazioni, al Garante, relative al trattamento dei dati, previste dall'art. 37, oppure in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante stesso, o ancora nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze, ovvero produce atti o documenti falsi.

Tale delitto, evidentemente, rappresenta una *parziale* riproposizione di quello previsto dalla formulazione originaria dell'art. 35 della L. n. 675/96. Attualmente, quindi, se è vero che, come accennato, è stata mantenuta la scelta — già operata nel 2001 — di depenalizzare l'omessa notificazione, è stata altresì confermata quella di far presidiare da sanzione penale la notificazione infedele. Ed anzi, come appena illustrato, sostanzialmente riproponendo il testo dell'art. 37-*bis* della L. n. 675/96 — introdotto, appunto, dal D.Lgs. n. 467/01 —, è stato assai ampliato l'ambito di penale rilevanza delle falsità commesse nei confronti del Garante. Inoltre, il dolo generico che caratterizza la fattispecie fa sì che sia sufficiente, in capo all'agente, la consapevolezza della falsità, delle notificazioni, comunicazioni, ecc., nonché, coerentemente con quanto generalmente ritenuto in tema di reati di falso[16], della loro idoneità (*ex ante*) a rivestire una apparenza ingannevole[17].

[16] Cfr. Cass. pen., sez. VI, 21 gennaio 2005, in *Ced Cass.*, rv. 231485.

[17] Cfr. Manna, *Codice della* privacy..., *cit.*, 27.

L'art. 169, invece, prevede la contravvenzione di omessa adozione di misure di sicurezza, la quale punisce, con l'arresto sino a due anni *o* con l'ammenda da diecimila a cinquantamila euro (risultando, dunque, eventualmente oblabile, *ex* art. 162-*bis* c.p.), chiunque omette — testualmente, « *essendovi tenuto* »: ma, chiaramente, solo chi è tenuto a fare qualcosa può omettere di farla — di adottare le misure minime, di cui all'art. 33, per garantire la sicurezza dei dati. Quali esattamente siano, però, tali misure minime non risulta in modo affatto chiaro ed incontrovertibile dal dettato normativo, per cui, al riguardo, può certamente lamentarsi un *deficit* di determinatezza, con violazione conseguente dell'art. 25 co. 2 Cost., che fa nettamente propendere per l'opportunità di depenalizzazione della contravvenzione in commento.

Ma, del resto, lo stesso può dirsi anche per il « delitto contravvenzionale »[18], di cui all'art. 170, che punisce, con la reclusione da tre mesi a due anni, chiunque — sempre, testualmente, « *essendovi tenuto* » — non osserva il provvedimento adottato dal Garante ai sensi: dell'art. 26 co. 2 (relativo ai dati sensibili), dell'art. 90 (in tema di dati genetici e donatori di midollo osseo), nonché degli artt. 143 e 150, afferenti, rispettivamente, ai casi di procedimento per reclamo e per ricorso. Medesimo destino, inoltre, dovrebbe spettare alle « *altre fattispecie* », di cui all'art. 171, sulle quali non si ritiene necessario spendere parole di commento, se non per ribadire la convinzione, più generale, di questo scrivente, relativa alla necessità dell'abbandono del modello puramente sanzionatorio del diritto penale[19], che, per di più, nel caso di cui all'articolo da ultimo in commento, è coniugato con sanzioni (eventualmente oblabili) davvero particolarmente lievi, e quindi ineffettive.

5. L'illecito trattamento dei dati personali.

Salvo che il fatto costituisca più grave reato, il delitto di trattamento illecito di dati — previsto, attualmente, dall'art. 167 del codice, e, in precedenza, dal citato art. 35 della L. n. 675/96 — punisce, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali, in violazione di quanto disposto: dall'art. 18 (che contiene i principi applicabili a tutti i trattamenti effettuati da soggetti pubblici), dall'art. 19 (relativo ai principi applicabili al trattamento di dati diversi da quelli sensibili o giudiziari), dall'art. 23 (secondo il quale, per il trattamento di dati personali da parte di privati o di enti pubblici economici, è necessario il previo consenso dell'interessato), dagli artt. 123, 126 e 130 (circa i dati delle comunicazioni elettroniche), nonché in violazione delle modalità di trattamento disposte dal Garante con il provvedi-

[18] In questi termini, si esprime, se pur in relazione alle fattispecie incriminatrici di cui alla precedente legge in materia, Torre, *La gestione del rischio nella disciplina del trattamento dei dati personali*, in AA.VV., *Il diritto penale dell'informatica…*, *cit.*, 267 s. In argomento, più in generale, si veda Donini, *Il delitto contravvenzionale*, Milano, 1993.

[19] Cfr. Plantamura, *Diritto penale e tutela dell'ambiente: tra responsabilità individuali e degli enti*, Bari, 2007, 143 ss.

mento di cui all'art. 129 (in tema di elenchi di abbonati)[20]. È inoltre importante precisare che, se il fatto consiste in una forma di trattamento diverso dalla comunicazione o diffusione, il fatto medesimo è punito, testualmente, solo « *se dal fatto deriva nocumento* ».

Allo stesso modo, sempre solo se dal fatto deriva nocumento e, comunque, salvo che il fatto in questione costituisca più grave reato, il secondo comma dell'art. 167 punisce, con la reclusione da uno a tre anni, chiunque, al fine di trarre per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto: dall'art. 17 (sul trattamento di dati, diversi da quelli sensibili, che però presenta non meglio precisati « rischi specifici »), dagli artt. 20, 21, 22 commi 8 e 11, 26 e 27 (circa i dati sensibili e giudiziari), dall'art. 25 (relativo ai casi di divieto espresso di comunicazione e diffusione), dall'art. 45 (sul divieto di trasferimento di dati all'estero).

Ebbene, in primo luogo si deve osservare che, siccome, ai fini della punibilità, è necessariamente richiesto l'accertamento di un nesso di derivazione, dal fatto, di un nocumento — accertamento che, chiaramente, si ritiene superfluo nei casi di pubblicazione e diffusione che, in sé, costituiscono un nocumento[21] —, si è di fronte a (tre autonomi) delitti posti a protezione, non già delle funzioni del Garante, ma dell'autonomo bene giuridico strumentale costituito dalla *privacy*, intesa nella sua accezione meta-individuale sociale, quale interesse al corretto trattamento dei dati. Risulta altresì evidente, tuttavia, che, sullo sfondo di tale tutela, si staglia il bene finale rappresentato dalla *privacy*, questa volta, però, intesa nella sua accezione individuale, quale « *right to be let alone* »[22].

In secondo luogo, invece, si deve sottolineare come il modello di diritto penale utilizzato, ovverosia quello parzialmente sanzionatorio[23] — caratteristico della normativa penale ambientale di alcuni importanti paesi europei —, il quale richiede, ai fini della sua integrazione, sia la lesione del bene giuridico tutelato che la violazione della normativa amministrativa di riferimento, risulti nel caso di specie particolarmente infelice. Si tratta, infatti, di una vera e propria « selva » di violazioni, spesso già in sé prive di determinatezza — come nel caso, già accennato, dei dati non sensibili, il cui trattamento, tuttavia, presenta dei « rischi specifici » —, e che, per di più, a loro volta possono anche rinviare ad altre normative, magari neppure puntualmente specificate.

---

[20] Veramente, con riferimento all'art. 129, il legislatore usa l'espressione « *in applicazione* », invece di quella « *in violazione* »: trattasi, evidentemente, di un *lapsus calami*, il quale, tuttavia, non può non destare un certo sconcerto, dato che è presente proprio nella principale fattispecie incriminatrice prevista.

[21] Con riferimento alla precedente formulazione dell'illecito trattamento di dati, è stato sostenuto che il nocumento — allora previsto come circostanza aggravante — fosse insito in ogni trattamento effettuato senza consenso, per cui, almeno in tali casi, la previsione dell'aggravante avrebbe perso di significato. Sul punto si rinvia a CAGLI, *La rilevanza del consenso…*, *cit.*, 297.

[22] Nello stesso senso, si veda MANNA, *Codice della privacy…*, *cit.*, 26. Sulla questione della c.d. « seriazione » dei beni giuridici, si rinvia a FIORELLA, voce *Reato in generale*, in *Enc. dir.*, vol. XXXVIII, Milano, 1987, 770 ss.

[23] Cfr.: CATENACCI, *La tutela penale dell'ambiente. Contributo all'analisi delle norme penali a struttura sanzionatoria*, Padova, 1996, 259 ss.; nonché PLANTAMURA, *Diritto penale…*, *cit.*, 160 ss.

Come nell'ipotesi paradigmatica del trattamento di dati illecito perché compiuto — da privati o da enti pubblici economici —, in violazione dell'art. 23, e cioè senza aver ottenuto il necessario previo consenso dell'interessato. Infatti, proprio questa che, a prima vista, sembrerebbe l'ipotesi più semplice, è complicata oltre misura dall'esistenza dell'art. 24, che disciplina, in deroga a quanto previsto dall'art. 23, una moltitudine di casi in cui il trattamento di dati personali può essere effettuato senza il consenso, e, dunque, nei quali non può ritenersi integrato il fatto tipico di cui all'art. 167[24].

Come ritenuto anche dalla giurisprudenza, secondo la quale, testualmente, « *non è configurabile* » il delitto in commento qualora non si realizzi la violazione dell'art. 23, pur in assenza di consenso, « *giacché tale previsione va interpretata ed integrata tenendo conto sia dell'art. 5*[25] *del codice, che dell'art. 24 della medesima normativa che, in deroga all'art. 23, prevede i casi in cui può essere effettuato il trattamento senza consenso* »[26].

Inoltre, ognuno dei casi previsti dall'art. 24, a sua volta, può contenere ulteriori complicazioni e rinvii, come nell'ipotesi di cui alla lettera *f*) dell'articolo in questione, la quale, se, in una particolare situazione, ammette il trattamento dei dati senza il consenso dell'interessato, lo fa, però, solo se lo stesso è stato comunque effettuato « *nel rispetto della vigente normativa in materia di segreto aziendale e industriale* ».

Chiarita la sostanziale indeterminatezza — e dunque, almeno sotto questo aspetto, la probabile incostituzionalità — delle fattispecie incriminatrici in commento, si deve ora analizzare più da vicino l'elemento che costituisce la vera novità, della formulazione dei delitti di trattamento illecito di dati adottata dall'art. 167 del codice, il quale, per il resto, ripropone

---

[24] Cfr.: Romano, *Teoria del reato, punibilità, soglie espresse di offensività (e cause di esclusione del tipo)*, in AA.VV., *Studi in onore di Giorgio Marinucci*, a cura di Dolcini-Paliero, Milano, 2006, 1721 ss.; Salcuni, *Natura giuridica e funzioni delle soglie di punibilità nel nuovo diritto penale tributario*, in *Riv. trim. dir. pen. econ.*, 2001, 131 ss.; Plantamura, *Alle soglie del falso*, *ivi*, 2003, 1252 ss.

[25] Tale articolo, infatti, delimita l'ambito di applicazione del codice in questione, stabilendo, tra l'altro, al suo terzo comma, che « *Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione* ».

[26] Cfr. Cass. pen., sez. III, 17 novembre 2004, in *Dir. int.*, 2005, 257 ss., con nota seguente di Manna, *Privacy on line: quali spazi per la tutela penale?*; in questa *Rivista*, 2005, 499 ss., con nota seguente di Di Ronzo, *Il trattamento illecito dei dati nella nuova disciplina*; in *Foro it.*, 2006, II, 46 ss., con nota contestuale di Chiarola, *Trattamento dei dati personali su Internet ed illecito penale*; in *Dir. pen. proc.*, 2006, 464 ss., con nota seguente di Salvadori, *Il trattamento senza consenso di dati personali altrui reperibili su Internet costituisce reato?* In particolare, tale ultimo Autore, alla nota n. 9 del suo lavoro, attribuisce *erroneamente* al Manna l'affermazione — ovviamente priva di fondamento alcuno, come puntualmente osservato dall'Autore stesso — secondo la quale « *in assenza della verificazione dell'altrui nocumento, derivante dal fatto, non sussistono gli estremi del reato di cui all'art. 35 l. n. 675/96* ». Tuttavia, tale affermazione era contenuta in un classico « specchietto redazionale », e sarebbe stato sufficiente leggere il commento a sentenza in questione, per trovarvi scritto, a pagina 265, che « *nella struttura della fattispecie « semplice » di trattamento illecito di dati personali, di cui all'art. 35 l. 675 … il nocumento rappresentava unicamente l'oggetto del dolo specifico perseguito dall'agente*, di cui pertanto non era necessaria la realizzazione ».

quanto già statuito dall'art. 35 della legge previgente. Trattasi chiaramente del *nocumento*, che invece, come accennato, era previsto solo come eventuale circostanza aggravante nel succitato art. 35 che, lo si ribadisce, prevedeva un delitto analogo, tant'è vero che, secondo la giurisprudenza, « *In tema di tutela penale della privacy, esiste continuità normativa tra il reato di trattamento illecito di dati personali aggravato dalla produzione di un nocumento, quale previsto dall'art. 35 l. 31 dicembre 1996 n. 675, e l'analoga figura di reato ora prevista dall'art. 167 del vigente d.leg. 30 giugno 2003 n. 196, in cui il nocumento non costituisce più circostanza aggravante ma condizione intrinseca di punibilità* »[27].

Ebbene, a parte la questione della continuità normativa (che comunque si condivide), ciò che più preme rilevare è che, secondo la Cassazione[28], il nocumento rappresenta una condizione obiettiva di punibilità intrinseca, e non l'evento del reato[29]. Tale soluzione era stata già anticipata da attenta dottrina, secondo la quale, giustamente, la natura di *cdp* (intrinseca: e quindi coperta dal fuoco della colpa[30]), propria dell'elemento in questione, risulta dalla contemporanea presenza del dolo specifico (anche) di recare ad altri un danno. « *Apparirebbe, infatti, quantomeno incongruo prevedere quale evento del reato proprio il fine (*rectius*: uno dei fini) perseguito dal soggetto, che, in quanto riconducibile agli stilemi del dolo specifico, non è, notoriamente, necessario che si realizzi ai fini della consumazione del reato* »[31].

Per altro, proprio allo scopo di superare tale difficoltà, e dunque, in definitiva, di poter attribuire la natura di evento al nocumento, è anche stata elaborata, in dottrina, una interpretazione, certamente suggestiva, secondo la quale, al nocumento stesso, bisognerebbe attribuire un significato diverso da quello proprio del « danno » che caratterizza il dolo specifico.

Il danno, cioè, dovrebbe essere riferito a degli interessati specifici, come confermerebbe la correlata espressione « *ad altri* », il nocumento « *sembrerebbe invece cogliere un ambito di realizzazione più diffuso ed indefinito, di natura meta-individuale* »[32]. Tuttavia, la (pur raffinata) interpreta-

---

[27] Cfr. Cass. pen., sez. III, 26 marzo 2004, in *Foro it.*, 2006, II, 46 ss., con nota contestuale di CHIAROLLA, *Trattamento...*, *cit.* La scelta operata dall'Autore di commentare, nella stessa sede, le due sentenze, risulta particolarmente appropriata in virtù della circostanza che, in due casi solo apparentemente analoghi, la medesima sezione della Corte di Cassazione è arrivata a conclusioni opposte sulla configurabilità del reato.

[28] Nello stesso senso, si veda Cass. pen., sez. III, 9 luglio 2004, in questa *Rivista*, 2004, 461 ss., con nota di SICA, « *Danno* » *e* « *nocumento* » *nell'illecito trattamento di dati personali*, *ivi*, 715 ss.; nonché in *Dir. pen. proc.*, 2005, 338 ss., con nota seguente di ANTONINI, *Il trattamento illecito di dati personali nel codice della* Privacy*: i nuovi confini della tutela penale*.

[29] In tal'ultimo senso, invece, si era espressa CORRIAS LUCENTE, *La nuova normativa...*, *cit.*, 631 ss. Si veda, inoltre, MAGRO, *Iternet e privacy. L'utente consumatore e modelli di tutela penale della riservatezza*, in *Ind. pen.*, 2005, 931 ss.

[30] Cfr. Corte cost., 24 marzo 1988, n. 364, in *Foro it.*, 1988, I, 1385 ss., con nota contestuale di FIANDACA, *Principio di colpevolezza ed ignoranza scusabile della legge penale: « prima lettura » della sentenza n. 364/88*; nonché in *Riv. it. dir. proc. pen.*, 1988, 686 ss., con nota contestuale di PULITANÒ, *Una sentenza storica che restaura il principio di colpevolezza*.

[31] Così, testualmente, MANNA, *Codice della privacy...*, *cit.*, 23. Tuttavia, anche accedendo alla condivisibile interpretazione del nocumento quale *cdp* intrinseca, nel complesso, residuano non poche perplessità sulla qualità della tecnica legislativa utilizzata all'art. 167.

[32] Cfr. TORRE, *Modelli di tutela penale della* privacy *in internet*, in *Dir. pen. proc.*, 2004, 233 ss., e, spec., 239 ss.

zione di cui trattasi, secondo la quale, in definitiva, il nocumento — inteso, appunto, quale evento del reato — dovrebbe ritenersi configurato « *laddove il trattamento illecito comporti un'alterazione degli equilibri giuridici ed economici fra poteri pubblici e privati nell'ambito di una società democratica e liberale* »[33], rischierebbe di condannare alla ineffettività il delitto in oggetto.

Mentre, qualora — in una prospettiva opposta — si ritenesse tale « nocumento diffuso » integrato da ogni lesione delle funzioni e dell'attività del Garante, probabilmente si finirebbe per offrirne sostanzialmente una *interpretatio abrogans*, perché già inclusa nella necessaria violazione della disciplina amministrativa di riferimento.

D'altronde, a proposito del concetto di nocumento, la stessa giurisprudenza si sta indirizzando nel senso, magari più « scontato », ma decisamente più valido, almeno da un punto di vista applicativo, di riferire il nocumento stesso al soggetto cui i dati trattati attengono, specificando, inoltre, che non ogni *vulnus* minimo alla *privacy* del soggetto può essere ritenuto sufficiente all'integrazione dell'elemento di cui trattasi, perché invece, a tal fine, a carico del soggetto cui i dati trattati si riferiscono, deve verificarsi un effettivo danno personale o patrimoniale[34].

Chiarito questo, si deve infine affrontare l'ultimo fondamentale problema in tema di trattamento illecito dei dati, ovverosia quello riguardante l'ipotesi — presa in considerazione nell'ultima parte dell'art. 167 co. 1. — in cui, testualmente, « *il fatto consiste nella comunicazione o diffusione* » (in tal caso, come accennato, la pena della reclusione è, nel massimo, maggiore di quella prevista nelle altre ipotesi di trattamento illecito di dati di cui all'art. 167 co. 1).

Ebbene, in primo luogo, si deve sottolineare che si condivide l'opinione dottrinaria, secondo cui il comma in questione prevede, in realtà, due distinte fattispecie, ovverosia quella di trattamento illecito dal quale deriva nocumento, e quella autonoma di trattamento illecito realizzato mediante comunicazione o diffusione[35], non sottoposto alla *cdp* del nocumento.

L'impostazione contraria, infatti, in virtù della quale si ritiene la previsione relativa alla comunicazione o diffusione una circostanza aggravante del trattamento illecito dal quale derivi nocumento, non sembra tener conto che l'aumento del massimo edittale nelle ipotesi di comunicazione e diffusione è proprio dovuto al fatto che, in tali casi, è *implicito* un rilevante nocumento, quantomeno sul piano personale, per il soggetto cui i dati si riferiscono, e dunque la *cdp* del nocumento risulterebbe priva di utilità selettiva.

Resta solo da specificare, allora, quale sia, all'interno della seconda fattispecie autonoma, di cui all'art. 167 co. 1, il ruolo della « *comunicazione o diffusione* », che, da parte di autorevole dottrina[36], si ritiene una *cdp* intrinseca. Tale opinione, però, probabilmente non appare condivisibile, da un lato, perché forse non tiene in debito conto la differenza, tra l'espressione « *se dal fatto deriva* » — che spesso caratterizza proprio le *cdp* intrinseche — e quella « *se il fatto consiste* », che sembra richiamare

---

[33] Così, testualmente, TORRE, *ult. op. cit.*, 241.

[34] Cfr. Cass. pen., sez. III, 9 luglio 2004, *cit.*

[35] Cfr. MANNA, *Il quadro sanzionatorio...*, *cit.*, 753.

[36] Cfr. ID., *ult. op. loc. cit.*

una particolare modalità dello stesso fatto tipico, e, soprattutto, dall'altro, perché non valorizza sufficientemente la circostanza che, ai sensi del citato art. 4 lett. *a*), la comunicazione e la diffusione di dati altro non sono che *forme* di trattamento dei dati stessi.

Ma se il trattamento (illecito) è la condotta tipica del delitto di cui trattasi, come può, allo stesso tempo, essere una *cdp*, ovverosia un avvenimento esterno ed ulteriore rispetto al fatto tipico? In definitiva, cioè, questo scrivente ritiene che, qualora la condotta di trattamento (illecito) di dati consista, in particolare, in quelle specifiche forme di trattamento costituite dalla comunicazione o diffusione, dei dati stessi, sia integrata l'autonoma, e più grave, fattispecie delittuosa di comunicazione o diffusione illecita di dati personali.

6. Brevi cenni comparatistici.

In Francia, come accennato, la materia del trattamento dei dati personali è disciplinata dalla L. n. 78-17, così come modificata dalla L. n. 801-2004, l'articolo 50 della quale statuisce che le infrazioni alle disposizioni della legge di cui trattasi sono previste e punite dagli articoli del codice penale che vanno dal 226-16 al 226-24. Tuttavia, nella stessa legge speciale è contenuto il delitto di cui all'art. 51 che punisce, con un anno di reclusione e 15000 euro di multa, l'ostacolo alle funzioni del Garante (*rectius*: della Commissione nazionale dell'informatica e delle libertà), posto in essere mediante l'opposizione alle missioni di controllo, il diniego o l'occultamento d'informazioni, o la comunicazione di informazioni false od oscure.

La tutela codicistica, invece — alla quale è dedicata una autonoma sezione —, si apre, all'art. 226-16, con un delitto di trattamento di dati illecito (perché svolto in violazione della disciplina amministrativa di riferimento), eventualmente anche colposo, che prevede le pene di cinque anni di reclusione e di 300.000 euro di multa. Più interessante, comunque, potrebbe apparire il delitto di cui all'art. 226-19 — sanzionato con le medesime pene succitate —, di trattamento di dati personali giudiziari o *sensibili*, e cioè tali da far apparire, direttamente o indirettamente, le origini razziali o etniche, le opinioni politiche, filosofiche o religiose, o l'appartenenza sindacale, o che sono relativi alla salute o all'orientamento sessuale. È vero, infatti, che tale delitto, tranne le eccezioni previste dalla legge, è integrato ogni qual volta il trattamento sia effettuato senza il consenso dell'interessato, ma è altrettanto vero che il delitto stesso è limitato ai casi di trattamento informatizzato. Tuttavia, quasi con un ripensamento, all'art. 226-23 il legislatore francese specifica che le disposizioni summenzionate sono applicabili anche al trattamento non automatizzato dei dati, la cui messa in opera non si limita all'esercizio di attività esclusivamente personali.

Chiude la sezione di cui trattasi l'art. 226-24, secondo il quale le persone giuridiche possono essere dichiarate responsabili penalmente — con la previsione di pene sia pecuniarie che interdittive —, in base alle condizioni normalmente statuite, per tale tipo di responsabilità, dall'art. 121-2, delle infrazioni previste nella sezione in questione.

In Spagna, invece, la citata legge organica n. 15/99 non prevede reati, ma solo illeciti amministrativi, divisi in tre livelli di gravità, a cui corri-

spondono tre livelli di pena pecuniaria. Non bisogna dimenticare, però, che nel codice penale[37] è previsto un titolo dedicato ai delitti contro la riservatezza, al diritto alla propria immagine e alla inviolabilità del domicilio. Ebbene, il primo articolo di tale titolo, ovverosia il 197 (rubricato « *scoperta e rivelazione di segreti* »), al suo secondo comma, punisce con la reclusione da uno a quattro anni e con la multa da dodici a ventiquattro mesi, chiunque, senza esservi autorizzato, si appropria, utilizza o modifica, in danno di terzi, dati riservati di carattere personale o familiare altrui, che sono registrati in schede o supporti informatici, elettronici, telematici, o in qualunque tipo di archivio o registro pubblico o privato. Le medesime pene, inoltre, si applicano a chi, sempre senza autorizzazione, accede ai dati in questione con qualunque mezzo, e a coloro che alterano o utilizzano tali dati in danno del titolare o di un terzo.

La pena, invece — ai sensi del terzo comma —, è della reclusione da due a cinque anni, quando i dati di cui trattasi sono diffusi, rivelati, o ceduti a terzi. Mentre, sempre secondo tale comma, è punito con la reclusione da uno a tre anni e con la multa da dodici a ventiquattro mesi chi, conoscendone la provenienza illecita, ed al di fuori dei casi di concorso, realizza la condotta precedentemente descritta, sostanzialmente « ricettando i dati ». Le pene fin qui prese in considerazione, però, in virtù dei commi 4, 5 e 6 dell'articolo in oggetto possono essere aumentate, o comunque devono essere applicate nella metà superiore dell'intervallo edittale, qualora i fatti siano compiuti dai titolari o dai responsabili dei dati, nel caso in cui trattasi di dati sensibili, e nell'eventualità in cui ricorra il dolo specifico del fine di lucro.

In fine, è interessante notare come nello U.S. Code[38] (al Titolo 18, sul diritto e la procedura penale, nella Parte I, relativa ai delitti) sia contenuto un capitolo (l'88) dedicato alla tutela della *privacy*, il quale è composto da un solo paragrafo (il 1801) che, però, contempla una ipotesi, testualmente, di video voyeurismo, analoga al delitto di interferenze illecite nella vita privata, come ricordato, previsto nel nostro ordinamento all'art. 615-*bis* c.p.

La tutela dei dati personali, invece, è affidata alle norme contenute in un altro capitolo (il 123) che, tuttavia, appare assai parziale, in quanto si riferisce al trattamento illecito dei soli dati personali provenienti dai registri di Stato dei veicoli a motore. Per cui, il primo paragrafo del capitolo in questione, ovverosia il 2721, si preoccupa di indirizzare il suo divieto di *intenzionale* trattamento illecito dei dati personali, appunto agli ufficiali, o impiegati, dei pubblici registri automobilistici, i quali, comunque, possono essere sanzionati solo con la pena pecuniaria (§ 2723).

Chiaramente, poi, al medesimo § 2721, è pure elencata una serie di casi in cui l'uso dei dati è ritenuto, invece, ammissibile, come nelle ipotesi di incidente stradale, o di furto d'auto, o di finalità giudiziarie, anche civili, oppure qualora vi sia il consenso scritto dell'interessato. Mentre, il § 2727 dichiara illegale, per chiunque, il fatto di ottenere o rivelare informazioni personali, contenute sempre nei registri in oggetto, a meno che, beninteso, non si versi nei casi consentiti dal citato § 2721. Altrettanto ille-

---

[37] Cfr. *Il Codice penale spagnolo*, intr. Quinterno Olivares, trad. Naronte, Padova, 1997.

[38] Cfr. *www.law.cornell.edu*

gale, poi, è commettere falsità al fine di ottenere i dati di cui trattasi. Forse, però, quel che più appare significativo della disciplina in commento è che, in tutti questi casi di illecito, per l'interessato è ammesso il ricorso alla *civil action* (§ 2724), e la corte distrettuale, nelle ipotesi di intenzionalità o di imprudente disprezzo della legge, può applicare i danni punitivi.

7. Rilievi conclusivi.

In conclusione della presente trattazione, si può affermare, con sufficiente sicurezza, che la tutela dei dati personali, nel nostro sistema, è caratterizzata da un ricorso eccessivo allo strumento penale, che è proprio, per altro, anche della normativa appartenente ad altre moderne ed avanzate democrazie occidentali. Probabilmente, cioè, si è di fronte ad un caso in cui, appunto attraverso il ricorso al diritto penale, si è voluta svolgere una attività « promozionale » del bene *privacy*, inteso nella sua accezione meta-individuale sociale. Alla base di questa esigenza, forse, può esservi stata la necessità di scongiurare il realizzarsi, tramite l'utilizzo delle nuove tecnologie informatiche, di un clima da « grande fratello », evocato, d'altronde, alla fine degli anni settanta del secolo scorso, dal citato « progetto Safari ». Attualmente, però, la materia avrebbe decisamente bisogno, soprattutto nella sua parte strettamente penalistica, di un'opera di ridimensionamento, in virtù della quale, in primo luogo, si depenalizzasse ogni violazione diversa dall'illecito trattamento dei dati. Anche quest'ultima ipotesi, tuttavia, meriterebbe di essere assai più circoscritta, rispetto a quanto avviene attualmente, innanzitutto specificando che la tutela penale dev'essere relativa esclusivamente ai dati afferenti alle *persone fisiche*.

Ma non finisce qui. Si è davvero sicuri, infatti, che si voglia sanzionare penalmente ogni forma di trattamento illecito? E non sarebbe meglio, invece, limitare la tutela penale, se non alle ipotesi di diffusione — il che sarebbe troppo riduttivo —, almeno solo a quelle di *comunicazione elettronica* di dati? Certamente, tali domande non sono destinate a trovare una esauriente risposta, da parte del nostro legislatore, quantomeno nell'immediato futuro. E questo è dovuto anche alla circostanza che il codice della *privacy* è troppo recente, perché se ne possa auspicare una profonda rivisitazione, se pur limitata alla sua parte sanzionatoria. Tuttavia, in questa sede è comunque opportuno sottolineare che la dottrina penalistica non può « arrendersi » a questo tipo di legislazione costruita tramite rinvii a catena, per cui, data la doppia presenza selettiva, da un lato, del dolo specifico, e, dall'altro, della *cdp* intrinseca del nocumento — la sussistenza della quale avrebbe ad ogni modo una sua utilità, appunto selettiva, rispetto alle ipotesi di comunicazione, e non di diffusione —, si potrebbe pure pensare ad una fattispecie incriminatrice di comunicazione elettronica di dati personali, relativi alle persone fisiche, finalizzata al proprio od all'altrui profitto, od all'altrui danno, punita se dal fatto deriva nocumento. La *cdp* intrinseca, però, potrebbe anche ritenersi superflua, nel caso di comunicazione elettronica di dati *lato sensu* sensibili.

Cogliendo, infine, alcuni interessanti suggerimenti provenienti, rispettivamente, dalla legislazione statunitense e da quella francese, si potrebbe introdurre, nei casi di illecito extrapenale, la possibilità di utilizzare lo strumento dei *danni punitivi* (di cui, da più parti, ultimamente si auspica

la « importazione » nel nostro sistema[39]); mentre, da un punto di vista più squisitamente penalistico, si potrebbe far rientrare l'ipotizzato delitto di comunicazione elettronica di dati, all'interno del novero dei reati presupposto, per la responsabilità da reato degli enti, di cui al D.Lgs. n. 231/01[40].

[39] Cfr.: STELLA, *Giustizia e modernità*, 3ª ed., Milano, 2003, 483 ss.; D'ACRI, *I danni punitivi*, Roma, 2005; PLANTAMURA, *Diritto penale...*, *cit.*, 107 ss., e ancor prima, pure per l'individuazione, nel metodo, di un limite massimo nella quantificazione dei *punitive damages*, MANNA, *Beni della personalità...*, *cit.*, 632.

[40] Non senza un certo anticipo, si era espresso a favore dell'introduzione di una responsabilità diretta degli enti, nella materia di cui trattasi, MANNA, *La protezione penale dei dati personali nel diritto italiano*, in *Riv. trim. dir. pen. econ.*, 1993, 179 ss., e, spec., 190.